HEALTH DATA ARCHIVING

Healthcare IT leaders discuss data archiving concerns and priorities

Archiving data from legacy systems is important in every industry, but especially in healthcare. Strong, secure data archiving capabilities are essential to every health system's ability to ensure continuity in care, protect patient safety, comply with regulations such as HIPAA and the Cures Act, reduce the costs of data storage, and minimize the risk of data breaches.

Yet some organizations are hesitant to retire their legacy systems, whether due to the perceived challenge of archiving these systems or the anticipated cost. A HIMSS 2021 cybersecurity survey found 73% of the health systems represented still operate legacy systems.

Recently, LDA convened a group of healthcare IT leaders from hospitals and health systems—from IT directors to senior managers of clinical systems and more—to explore common pressures that influence the decision to archive and what they look for in an archiving partner.

1 LEGACY DATA SECURITY IS A TOP CONCERN

80 percent of the leaders rated security as their top consideration in selecting a healthcare data archiving partner for their financial, clinical, and operational systems.

It's easy to understand why: Among HIMSS survey participants, 39% say maintaining the security of legacy operating systems is a challenge, while 337 healthcare organizations experienced data breaches in the first half of 2022 alone, affecting more than 10 million healthcare records.

It's one reason why healthcare leaders use third-party security assessment consultants to evaluate their healthcare data archiving partner's security record and its approach to protecting legacy healthcare data.

"I've got [internal] security covered. We're a 98 on SecurityScorecard and pretty high on BitSight," shared one IT director of revenue cycle systems.

"If I'm going to give you data, you have to be able to take care of it."

Everyone touching the data should be held to the same security standards: A vendor's approach to protecting data access—including among the vendor's employees —should apply to its third-party partners as well. And it should be demonstrable.

"I'm not concerned about the machines and staff I control. I'm concerned about the ones I don't."

Transparency, too, is crucial to the archival process. Leaders want to know their data is being archived quickly and appropriately and that the right measures are in place to protect their data at each stage in the process.

Other IT leaders expressed concerns around the quality of third-party security assessments. For example, one leader described a recent internal and external penetration test as part of the institution's compliance with its cyber-insurance requirements. When he read the firm's report, there were issues with the findings, which included a false positive report. "Once I had them re-run the assessment, our rating changed to an appropriate level of risk, as it should have. But had I not known what I was looking at when I looked through that report, that insurance company would have had a false impression of my organization's security practices.

"At the end of the day, I don't know the quality of vendor that's being used to do security assessments."

Also keeping IT leaders up at night: the reliability of data security firmware and software.

One leader explained the one thing he watches closely on every vendor is security patching—making sure their data archiving partner is applying security patches monthly and keeping everything up to date.

2 GREAT RESIGNATION DRAINS HIGH-LEVEL IT EXPERTISE

Although IT staffing issues weren't a top-priority focus for this group of IT leaders, the impact of senior-level vacancies or turnover garnered a significant share of the discussion.

One IT leader shared: **"Internal staffing is my lowest concern"**—a sentiment echoed by other leaders, particularly in a growing remote work environment, which has been a benefit to their IT departments. Leaders are now able to hire out-of-state employees, opening their pool of IT candidates and offering redundancy in staff.

Instead, turnover on the vendor side and among senior IT leaders is a growing concern. Vendor turnover creates significant risk for health systems because it results in a lack of institutional knowledge around how to retire legacy systems, much less a wide variety of systems. Additionally, loss of internal IT leaders, such as CIOs, due to the Great Resignation limits health systems' ability to respond with agility when legacy systems need to be retired. This is especially true when a change in internal leadership is combined with vendor turnover.

"The difficulty on our side has been with the patchwork of legacy systems that we have to decommission and the absence of knowledge around those systems," one leader in the group observed. "There are multiple different systems across the board, and ensuring we have in-house leaders who know those systems and can help with the extraction and validation of data from these systems is a concern of mine."

3 COST CONTAINMENT PLAYS SIGNIFICANT ROLE IN DATA ARCHIVING DECISIONS

For some systems, cost considerations play a significant role not just in determining whether to retire legacy systems, but also how. It's a finding that also was expressed in the HIMSS report, where 47 percent of respondents say budget challenges force leaders to choose which systems to maintain, upgrade or acquire, presenting security issues for these organizations.

"What I'm hearing is that the struggle for cost containment is our health system's No. 1 problem," one leader explained. "It's difficult to make the case to keep paying what I'm paying now for archiving if I'm receiving the same level of security for my investment than if I had simply kept the data in the legacy system.

One trend leaders are seeing is an increased ability for health systems to shift budgeted capital expense dollars from one project to another throughout the year, rather than firmly sticking to an "X capital expense dollars go to Y initiative" approach. In doing so, organizations gain the ability to direct dollars where they are needed, as they are needed—including for healthcare data archiving. When combined with flexible pricing models for healthcare data archiving, this supports a more agile approach to legacy system retirement that some systems might not otherwise have been able to afford.

"If there isn't a marked increase in data security through data archiving, why don't I just leave the data where it is instead of archiving it?"

4 HEALTHCARE M&A PUSHES DECISION-MAKING AROUND LEGACY DATA TO THE FOREFRONT

Strategic healthcare deal volume is down but not dead—and with it comes a host of considerations around how to archive legacy data for a smooth and compliant transition: for staff, for systems, for budgets, and for critical data.

When it comes to retiring legacy operating systems after a healthcare merger or acquisition (M&A), the consensus is that it can be tricky.

"Our system keeps adding new contracts and new physician organizations, and the contracts that get written are sometimes vague," one leader shared. It's an issue of either, 1) We're taking your practices and your data; or 2) You're keeping your own data. In either instance: Who's responsible for extracting, validating, maintaining and protecting that data? The answer is not always clear, according to leaders, and this can compound all three of the aforementioned challenges, including staffing, cost, and security.